User-centric Networking Living-Examples and Challenges Ahead

Rute Sofia[⋆], Paulo Mendes, Waldir Moreira

COPELABS, University Lusófona, Lisbon, Portugal
{rute.sofia,paulo.mendes,waldir.moreira}@ulusofona.pt

1 Introduction

Throughout the history of the Internet, several technologies and networking architectures have emerged, some of which have been widely deployed, and others have only made its reach to niche markets. Some generic cases that can be cited are multicast, IPv6, java, or even C++. Clearly, the adoption of such technologies relates not only to technical merit but also to a variety of parameters such as ease of deployment, or even interest of potential market stakeholders.

In what concerns the specific case of wireless networks which today abound as local access networks with limited mobility support, their utilization in more disruptive scenarios is yet to see a mass deployment. For instance, the *ad-hoc* wireless architecture concept has emerged around 30 years ago and is yet to see a generalized deployment.

The lack of a mass deployment of ad-hoc networks may possibly be due to the fact that entities managing different networks (be it individuals or large organizations) lack clear incentives to participate in the creation of ad-hoc wireless networks. The result of this is actually the rise of simpler and more autonomic wireless architectures, *mesh networks*, in which all devices are static (placing lower technical challenges) and normally belong to the same administrative entity (thus reducing the adoption problem). Previous experience therefore shows that spontaneous deployments of infrastructure, mesh or ad-hoc wireless networks are changing the perceived applicability of new types of wireless emerging architectures, but there is still not a clear perception on how such adoption may progress, nor a clear perception on what are the incentives (from a social, economic and also technical viewpoint), both from an access and end-user perspective, to adhere to these networks. Last but not the least, there is also not a clear perception on the dynamics of these networks.

Despite the aforementioned aspects, a recent trend related to autonomic wireless architectures is giving rise to wireless community initiatives with the purpose to provide broader connectivity. In these type of architectures (*User-provided or User-centric networks, UCNs*) [22], **users and/or communities share subscribed access in exchange of specific incentives**.

[⋆] Corresponding author. COPELABS, University Lusófona, Building U First Floor, Campo Grande 388, 1749-024 Lisboa.

UCNs disrupt Internet communication models in several ways. Firstly, any regular end-user device may behave as supplier of Internet connectivity and other services, and consequently, the user device becomes part of the network. In contrast, the architectural core of the Internet, the end-to-end principle [10], describes a clear splitting between network and end-user systems. Secondly, UCNs grow spontaneously based on the willingness of users to share subscribed Internet access. Thirdly, connectivity is expected to be intermittent given that UCNs are spontaneously deployed. These are some intuitive aspects which show that UCNs are a new paradigm at least in terms of Internet connectivity models. However, there is today still not a clear understanding of the extent and of the impact that this rising trend may have in the Internet design. As an initial step towards a better understanding of what such impact may be, this paper is focused on an analysis of existing examples of UCNs, their operation as well as advantages and disadvantages. Hence, the paper is organized as follows. Section 2 describes related work. Section 1 goes over the different examples of UCNs categorizing them according to their main properties. Then, section 6 provides a list of derived assumptions and requirements based upon the four main UCN properties. Conclusions are provided in 7.

2 Related Work

The quickest distinguishable feature of UCNs is Wi-Fi sharing. Different terms found in the literature that point to the UCN concept are *social wireless networks*, *community Wi-Fi sharing*, and also *Peer-to-Peer Wi-Fi*.

The technical benefits of Wi-Fi sharing have been analyzed to some extent [14,26] and measurement results show that such sharing is a cost-effective solution in particular for densely covered areas. These contributions relate only to specific examples of controlled deployment of public wireless networks.

Camponovo and Cerutti provide an analysis of regulation aspects concerning hotspot sharing [**?**]. The authors analyze hotspot sharing based on two regulatory (European) regimes, addressing different sharing models and explaining regulatory gaps.

Specifically concerning UCNs, user-centric wireless models [22] show that today the Internet end-user is already not only a consumer but also a provider of Internet services in the sense that he/she can share his/her subscribed Internet access based upon specific (community) sharing incentives.

Our work provides a reality-check about the current status of UCNs by analyzing real deployment cases and by contributing to a better understanding and characterization of this emerging type of network architecture.

3 The Global Concept of a User-centric Network

This section provides a characterization of user-provided networks, including a set of assumption and requirements. To clarify main differences against other autonomic networks, the section also provides a comparison of connectivity features for user-provided networks against ad-hoc and other forms of multihop networking.

A UCN may be represented by a time-varying graph where *nodes* are wireless devices belonging to Internet users (individuals or communities), and where *edges* represent trust associations. The edge cost is a measure of the trust association strength. From a pure connectivity perspective, nodes have two roles: *regular* and *gateway.* Regular nodes use network resources provided by a gateway. Gateways provide networking services to a specific community of users, e.g. share bandwidth and provide mobility management solely based on their owner's (the *micro-provider, MP*) subscribed Internet access or in a coordinated way with one or several access providers. From a management perspective, a third entity integrates the UCN concept, the *Virtual Operator (VO).* The VO is a role that provides some form of coordination (e.g. access point registration) to specific UCN communities without owning a specific infrastructure nor providing services. Therefore, a VO is simply a role assumed by an entity, by an *Internet Service Provider (ISP)*[1] , or by a *Service Provider (ASP).*

User-centricity is a key aspect of UCNs: these architectures emerge based on user empowerment made possible by the ease deployment of new types of wireless architectures and by the user willingness to cooperate due to some form of communal or individual benefit (*incentive*). In addition to user-centricity, UCNs hold four other properties: *network resource sharing*, *cooperation*, *trust*, and *self-organization.*

Network resource sharing today reflects mostly Internet access or connectivity sharing. However, as these architectures evolve, we will likely observe sharing of additional network resources (e.g. energy) or of additional network services (e.g. mobility management).

Cooperation relates to the user's willingness to participate in UCNs, both sharing and profiting from available resources. Incentives to cooperate can be related to trust (e.g. social association), to some form of compensation (e.g. broader Internet access), or even to a more efficient network operation.

Trust management is today performed by having users signing up to a "community". However, to create UCN secure environments, user identification and traceability are issues that have to be addressed. Hence trust management relates to three main security concerns: *i) assist users in terms of traceability; ii) guarantee user privacy; iii) provide data confidentiality when/if necessary.*

Self-organization relates to the capability to coordinate connectivity in scenarios where it can hardly be predicted given that it is based on the user's willingness to cooperate or adhere. In regards to self-organization, a key aspect is that UCNs rely on existing (private) deployments. For instance, in a campus it is likely that a UCN would rely on the existing Wi-Fi infrastructure mode. While within a village, a mesh solution could make a more adequate UCN.

[1] Internet access or connectivity is here defined as a networking service consisting of IP address space allocation, Domain Name Service and routing assurance.

3.1 UCN Taxonomy

The roles of the UCN stakeholders (users, MP, operators) and their relationships shape the Internet design, as these relationships impact the communication in ways that were not foreseen, e.g., by placing both the upstream (from user to network) and downstream (from network to user) flows at an equal level. To better understand what may be the impact of UCNs over the Internet, we analyze some of the most representative UCN examples as of today, and categorized them into five different sets: hotspot UCNs; mesh UCNs; Social networking UCNs; Mobile/Provider UCNs.

Hotspot UCNs represent most likely the majority of UCNs around us. In this category, UCNs are built upon existing Wi-Fi hotspots. Hence, hotspot UCNs are based on Wi-Fi infrastructure-mode, where an *Access Point* (AP) mediates all communication to and from a set of end-user devices. Users adhere to hotspot UCN models due to roaming incentives: a user shares his/her Internet access subscription in exchange of roaming across other hotspots shared within the same community.

Mesh UCNs are possibly the oldest UCN category. It should be noticed that UCNs based on mesh relate only to *user-centric mesh networks*, given that communities of users autonomously deploy the network. The wireless infrastructure is often deployed by the community to allow Internet expansion in relatively large areas. Incentives relate to low-cost Internet expansion (capilarity) and not so much with roaming.

Social networking UCNs rely on social networking to seamlessly distribute Wi-Fi credentials and to allow UCN expansion. The MP shares Internet access based upon credentials that he/she controls and in situations where the gateway can be simultaneously used by different users, as happens in a household.

Mobile/provider UCNs are the most recent UCN category. The potential of this type of UCNs is still to be unveiled but what is clear is that the solutions here described will drive the deployment of UCNs. In this category, the network is formed anytime/anywhere by users according to their needs and following the subscription rules of their cellular providers. Mobile-based UCNs are often provided by operators due to offloading reasons, as a way to lower Capital EXpenditures (CAPEX).

4 UCN Living Examples

Finally, *Provider-based UCNs* are examples of concrete business applications of UCNs where the provider (access or service) is also a *virtual operator (VO)*.

This section provides an overview of today's living examples of UCNs. Such examples have been analyzed and grouped into different categories according to their operandis mode, and the proposed categories are illustrated in Figure 1. As illustrated we consider five main models to categorize living examples of UCNs. The next sections will describe each of these categories, addressing operation for each of the examples, and summarizing the main aspects for each category.

Within each category we have grouped the known examples of UCNs. Then, within each category examples of operation as well as a description of the main features are debated. Such features contemplate resource management, cooperation incentives, mobility management, security aspects, and additional features which are relevant to cite as differentiators.

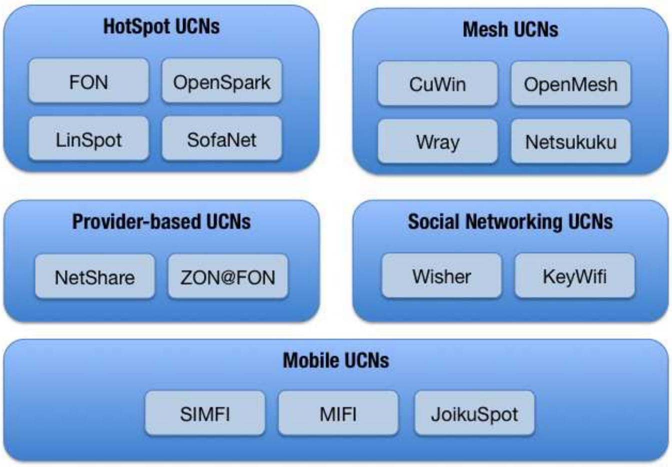

Fig. 1. UCN categorization.

4.1 Hotspot UCN Model

Hotspot UCN models rely on regular hotspots owned by users (or available in public spaces) and give the opportunity for users belonging to the communities coordinated by VOs or ISPs to take share subscribed access and to take advantage of such sharing. In this category, the architecture relied upon corresponds to the regular infrastructure-mode of Wi-Fi, where an access point mediates all communication to and from stations. The access point (co-located with an access router) is normally provided by the VO. Moreover, the VO takes care of authentication of users within the community it coordinates. Today, most households represent a hotspot UCN.

The incentives for this category relate with roaming: a user shares an already subscribing access in exchange of roaming across other shared accesses. It should be remarked that a user is only entitled to roaming if i) he/she acquired a gateway to a VO; ii) such gateway becomes active and is registered (on the VO backend systems) as a shared hotspot.

In this category, there is no end-to-end data confidentiality nor privacy. Moreover, the MP is the responsible for any traffic to the access. In other words: access providers can only consider accountable the MP: any violation of the subscribed access is input ed to the MP.

FON FON [13] is one of the most concrete and successful examples of a hotspot UCN model, and in . As of July 2013, FON claimed to have the largest Wi-Fi network with over eight million hotspots worldwide.

In order to be part of FON, all any user has to do is to register as part of the community, which implies obtaining credentials. In addition the user has to acquire a FON "social" router (FONERA). This is in fact an Access Point/router (AP) which is ready to allow Internet connectivity sharing and that will also be the basis for the free hotspots that are available to all FON users. Each FON social router is associated with specific user (username/password) credentials and as soon as it gets registered, it becomes a FON access point. The access to the FON social router is performed by the regular redirection to a Wi-Fi portal: each time a user is within the range of a social router and connects to the given signal, the browser is automatically redirected to the main portal page, which asks for the user's credentials.

Users that register in FON are expected to already hold an Internet access subscription. Hence, FON is not an operator nor a *Service Provider (SP)*. FON simply provides a box and a virtual registration to a community, and hence is here coined with the notion of *Virtual Operator* (VO).

FON subscribers are then split into two categories, *Linus* or *Bills*. Linus are users that hold a broadband connection and a FON social router. By means of acquiring the social router, they are entitled to roam across the FON Wi-Fi hotspots for free. This is the regular case of a residential user that simply wants to have the possibility to roam freely. Here, the incentive to share is simply broader roaming.

Bills are users that want to do more than roaming, namely, they are looking for a financial incentive to use FON. Bills receive 50% of the net revenue due to end-users (*Aliens*) that access FON by mean of previously acquired FON passes. Such end-users then access FON by means of the Bills' APs. In addition, FON gives Bills the means to personalize their access points and sign-in pages - Bills can then advertise their products and services within their neighborhoods. Overall, only Linus users have unlimited/free access to FON APs. Bills in contrast have to pay the access as normal users (but receive part of the income).

Today FON deploys their firmware on a large variety of low-cost APs, ranging from Linksys to Netgear. The firmware is based on the OpenWRT operating system.

Operation Let us provide a concrete example for Bob, a user that wants to use FON to be able to profit from broader roaming. Bob goes to the FON site and registers freely as a new user providing the regular details such as e-mail address, postal address, etc. Upon registration, Bob becomes an Alien, i.e., Bob is registered but is not yet a FON subscriber. In order to become a Bill or Linus, Bob needs to acquire a FON social router (FONERA) and to activate sharing, i.e., to establish a *FON spot*.

Upon arrival of the new AP to his house, Bob connects it following FON's guidelines. Bob then enables sharing and registers its FON social router on the FON online account, thus becoming a Bill and obtaining access in any FONSpot worldwide.

When Bob roams and wants to access other FonSpots, he has simply to enter his credentials on the captive portal of FON. There is no security however, for the users profiting from shared connections.

In regards to resource management, FON provides very simple support, which only considers a simple priority scheme to take into consideration potential downstream and upstream restrictions. More relevant is the fact that a MP can limit (manually) the amount of bandwidth being shared.

Incentives to cooperate in FON are two-fold. Broader roaming is no doubt the main incentive to address. In addition and specifically for the case of Bill users, there is a financial incentive: FON allows Bills to keep half of the voucher generated revenue. Mobility management is not integrated in FON. The user can roam but there is no session continuity, nor any guarantees in terms of nomadism.

In terms of security, FON protects the wireless connection of the MP with regular means, e.g., WPA, WPA2, WEP. The shared access is, however, open.

Additional features supported by FON that are relevant to cite are that sharing is an optional feature. In order to roam a user has to acquire an AP from FON. However, if that AP is not active, the user can roam within the FON community. Moreover, the last APs incorporate a number of collaborative tools (e.g. Twitter, bitTorrent clients) and the user can download content from the Internet independently of his FONERA being or not being active.

In terms of policing and monitoring, FON equipment provides regular traffic management statistics (but does not differentiate between MP and shared connections.

OpenSpark Being a predecessor of FON, OpenSpark [15] provides a similar type of architecture in Finland. OpenSpark is managed by MP-MasterPlanet Ltd, a Finnish ISP/WISP which manages the Wi-Fi network SparkNet. OpenSpark was born of SparkNet, and follows a model where the usage incentive is free roaming. Being a simple case of FON, OpenSpark provides less features than its peer.

Generic Operation Similarly to FON, in order to use OpenSpark Bob needs to have an Internet access subscription and to acquire an AP that has been personalized for use in OpenSpark. Bob then needs to activate the AP at home, to take care of its configuration, and to register itself (by means of the new AP and of the captive portal of OpenSpark) as an OpenSpark user.

OpenSpark does not provide any resource management, and the single type of incentive is broader roaming for users adhering to the community. Similarly to FON it does not contemplate any mobility management features. A key differentiator aspect to FON is that sharing is mandatory: the acquired APs must be up all times. Another differentiating aspect is the fact that OpenSpark allows expansion of hotspots by means of bridging between multiple APs (which will be seen as a single virtual AP).

LinSpot LinSpot [11] is intended to be an easy off-the-shelf solution that allows a user to profit from an already existing subscribed Internet access, by turning the local AP into a paid and profitable hotspot. Compared to FON's 'Bill' model, LinSpot is cheaper to setup, as it is software-based and does not require the purchase of new hardware. On the other hand the MP must have an existing (compatible, open-source) AP/AR and a computer with an Ethernet interface. This computer will have the LinSpot software installed and is the manager of a LinSpot hotspot - the computer must be up all times. All the APs in the LAN segment therefore become LinSpot APs.

The business model of LinSpot is that LinSpot fixes the prices of Internet access in LinSpot-enabled APs. These prices are said to be half of those of commercial WISPs. The MP gets 85% of all profit, being that the remaining 15% goes to LinSpot. Payments are done via the PayPal system and profits are immediately transferred to the MP's account.

In its current version, LinSpot is available only to MacOS X operating system and does not support any form of wireless security.

Generic Operation Firstly, Bob checks that his computer is connected to his AP/AR through an Ethernet cable and that the computer is configured to have a static IP configuration. In addition, in his router, DHCP, DNS, and security must be disabled (as LinSpot packs a DHCP server) .

Then Bob is ready to download the LinSpot software (currently only available to MacOS X) and follow the installation instructions. If not already registered in PayPal, Bob must create an account and register in LinSpot, in order to receive the payments. After this setup, anyone connecting to this access-point will be redirected to a web page with the billing information and, after paying the fees, allowed to use Bob's Internet access.

This means that every device in Bob's LAN will be redirected to this page. To avoid this, the LinSpot system is prepared with a free-access list with devices that are allowed to connect freely. Bob must add to this list every other computer he might have.

By installing LinSpot, Bob is opening a specific LAN (e.g. his home hotspot) to everyone around. Together with the fact that no encryption is being used, this means that Bob must be careful with the resources he is sharing (e.g. files and printers) because everyone will have access to them. Furthermore, Bob will have to leave his LinSpot-enabled computer turned on all the time, or his hotspot won't work.

The cooperation incentive for LinSpot is financial: an MP can get 85% of revenue for users that rely on his/her hotspot. Moreover, roaming is also considered as an adhesion incentive, for users willing to pay monthly access fees.

LinSpot provides no security at all. As additional features, LinSpot incorporates logging, as well as billing reports which are provided to MPs.

SofaNet SofaNet [?] is one example of a UCN model in which a user needs to pay to have connectivity. To be able to use Internet connections made available by SofaNet members, one has to buy a flat rate voucher "Zeitflatrate" with SofaNet for 15 Euros. Vouchers can be used for 90 days, around the clock, but they come with a transmission volume limit.

The major condition to become a SofaNet member is to have an Internet subscription from T-Com or a reseller such as AOL, Freenet, or 1&1. SofaNet members can use their own DSL identification for their own Internet access. A new DSL identification, bought from SofaNet, will be used by guest users. Both DSL identifications can be used simultaneously over the same DSL connection. For that, two WLAN routers need to be configured with the different DSL identifications. The DSL identification (e.g., PPPoE identification) identifies the user as well as the tariff (e.g. flat rate), which allows the SofaNet member to still use its own tariff plan, while guest users are allowed to use a different one. Any SofaNet member has to respect the SofaNet rules and must behave according to the conditions of the DSL operator. SofaNet is registered with the Federal Network Agency in Germany and provides the required storage of connection data. A SofaNet member is responsible must not give Internet access to anonymous users and should encrypt all the traffic.

For guest visitors, SofaNet relies on the pre-paid model. Pre-paid packages go from 1-2,5 Euros for 500 MByte transmission volumes for 24 hours to a 15-37,50 Euros package with 6 Gbyte volume for 90 days.

The major difference to previous examples (such as FON or OpenSpark) is that normally UCN hotspot models are directed to communities of users willing to roam for free, and outsiders have to pay for Internet access. In contrast, SofaNet members always pay for Internet access, although it is only 17 cents a day. Moreover, while the core business of FON is to sell their hardware (Foneras), SofaNet sells DSL identifications. With the usage of two different DSL identifications, it is easier with the SofaNet model to identify who is using the shared Internet access (the MP or the guest users). It should be noticed however that their model of operation is tied to German regulation, where there is still a clear splitting between the access line and the Internet services subscriptions.

Generic Operation To become a member of the SofaNet community, Bob first needs to buy a DSL connection from T-COM or a T-COM reseller. Hence, subscribers of other DSL operators in Germany, such as Arcor, Alice, Netcologne, and Versatel cannot become SofaNet members.

Bob must use its old DSL identification, while a new SofaNet DSL identification is to be used by guest users only. Once Bob gets its T-COM DSL connection and DSL identification, he has to buy two APs from SofaNet. One AP will be used by Bob only (protected with WEP/WPA) and the other is to be used for Bob's guests (open access). Both APs are expected to be connected to the same

DSL service (e.g. by means of a switch). Therefore, there is a physical traffic separation up to the APs that Bob acquired. Nonetheless, the wireless link for guests is unprotected.

Resource management can be supported by SofaNet by deploying two VPNs to the different APs. In terms of cooperation, roaming is again the main incentive provided. In addition, there is a financial incentive which gives SofaNet members the possibility to provide their own pricing model to guest visitors. Security aspects in SofaNet can be provided end-to-end (by means of VPNs and of DSL identification). By default the access for guests is left open. An additional feature to state is that members are offered 1Gbyte free traffic volume per month as incentive for roaming, as long as the user keeps the hotspots active more than 95% of the time.

4.2 Social Networking UCN Models

Social networking UCN models are examples of UCNs which rely on social networking aspects to distribute Wi-Fi credentials and to allow connectivity models to expand. The user therefore shares connectivity for which credentials are known and also for situations where the AP can be used simultaneously, as happens for instance at a residential household.

In this UCN category, there is still a VO which is responsible for backend management, mostly to register shared APs and to take care of the basic authentication. The MP relies on his/her own equipment to allow the sharing to happen, but however, such sharing is completely independent from the existing connectivity model and also from the existing wireless architecture.

Wifi.com Wifi.com[2] [25] is a brand for a UCN concept which goes a step further than FON in terms of empowering the end-user as connectivity provider, given that it bypasses the need to acquire hardware: Whisher's functionality is purely software-based and integrated into the end-user device. By relying upon a specific client software component (plugin[3]), Whisher gives the means to establish shared connectivity among users that belong to the social sphere of an MP. The Whisher plugin basically gives an MP the possibility to exchange, in a secure way, Wi-Fi credentials of an AP the MP controls to users from his/her social network(s). Connectivity sharing therefore follows a social networking model.

Wifi.com has three flavors of access grant, namely *public*, *buddies-only* (currently unavailable), and *private*. As its name suggests, public access grant allows anyone to use the hotspot as long as he/she has the Wifi.com client software and a registered account. For the case that the owner is still not comfortable about fully sharing his connection, he can provide access to only his family and friends through the buddies-only option. This option is also useful in the case of a small network among neighbors. For that, the owner has to add these users to his buddy list, and only the users on this list will be allowed to access the

[2] Formerly known as Whisher, Wifi.com is a brand reselling for the plugin Whisher.

[3] Currently only available for MacOS and Windows XP.

hotspot. As for the private option, only users set as VIP will be able to access the hotspot. In order to add a user to the VIP list, the owner of the hotspot must select them from the local Wifi.com users' list. Such option is available for the case when the owner wants to have the most of the bandwidth available to him, but without letting other important users (i.e. the VIP ones) without access.

The owner of the hotspot is responsible for setting security measures (e.g WPA/WPA-2, WEP) for his network. With that, the Wifi.com software will allow users access but without letting them know about the key.

Generic Operation Bob goes to the Wifi.com site and downloads the Wifi.com plugin for his machine, installing it. Once active, Bob is asked to register (obtain username and password) on Wifi.com. After registration, Bob provides information concerning the hotspot(s) he is willing to share, by issuing a specific identifier and a welcome message to other users belonging to his Wifi.com social network(s) . The connection sharing is managed automatically according to the levels of trust specified by Bob, and the Whisher manager provides secure connections to all users that Bob is sharing connectivity, by means of WEP.

As mentioned, only the owner of the hotspot (Bob) can decide who is going to be allowed to access his hotspot. Another interesting feature is the ability to be connected in areas where there is no other users sharing connectivity. This is possible through the partners registered (e.g., Starbucks, Accor hotels, Best Western hotels) that offer connectivity at a very reasonable price. All the user needs is charge his account with premium Wi-Fi minutes (wifi out credit in whisher) which will be used in a per-minute based form according to the needs of the user. it should be noticed that Wifi.com does not allow simultaneous access, given that it inherits the provided access rules - there is no connectivity model change.

Wifi.com simply relates to the exchange of credentials and therefore there is no concern in terms of resource management. However, the MP can trace the usage of his/her shared hotspots and can block greedy users from accessing a hotspot. Moreover, the MP can also define the maximum amount of bandwidth he/she is willing to share with each category of user. Incentives to cooperate are again related with broader roaming only. In terms of security aspects, there is a clear bet on security, given that the credentials of shared hotspots are only known to the MPs and are exchanged securely.

Key WiFi KeyWiFi [12]is a service provided by KeyWiFi LLC, New York, USA. KeyWifi has as mission to provide low cost broadband Internet access connections through a provisional patent-pending wifi sharing platform. In its essence the purpose is, as WiFi.com, to provide WiFi credentials to users roaming. KeyWiFi appeals to the regular end-user willing to become an MP and to get some profit out of such sharing. The argument of KeyWiFi relates to the unused spectrum available around, in particular in dense areas.

KeyWifi follows an ebay philosophy in terms of shared keys. Users willing to share their access (and to get revenue out of such sharing) register in KeyWifi as suppliers (MP). KeyWifi provides suppliers with a specific Keywifi key for each hotspot that the MP registers. The MP also pays KeyWifi $9.98 per month. Users that are willing to profit from KeyWifi shared hotspots will pay also $9.98 to KeyWifi, but two thirds of the fee will go to the user sharing a hotspot. KeyWifi therefore expects to be a catalyze for sharing of hotspots that today are simply private.

Generic Operation Bob has wireless Internet access both at home and at office by means of two different APs. Bob normally uses Internet access in his office during the morning, and during the afternoon and evening, he goes back home. Hence, both APs are in average unused 50% of the time. Bob therefore decides to make some profit out of it and joins (registers) on KeyWifi, agreeing to pay 9.98 $ per month. He registers both his home and office hotspot in KeyWiFi, and users belonging to the KeyWifi community (also registered) can access his shared hotspots. Then, registered users of the KeyWifi community can access Bob hotspot. Two thirds of their Keywifi monthly fee then go to Bob.

Being a very recent model, there are still a few open issues. For instance, simultaneous use of several hotspots by a single user requires some management in terms of the revenue obtained by the MP.

4.3 Mesh-Based UCNs

Mesh-based UCN models are examples of UCNs based on mesh networks and hence are possibly the oldest way to deploy the UCN concept. The wireless architecture is mesh-based but the deployment itself is performed by communities of users. Hence, VOs in mesh-based UCNs are municipalities and also even specific communities of users. Also, the MP tends to be the VO for this category, as shall be explained.

In this category, the wireless infrastructure is often deployed by the community to allow Internet expansion of already existing places. The incentives relied upon in this category relate often to Internet expansion at low-cost and not so much with roaming.

Wray Village The Wray village project [24,3] was born from University of Lancaster Wray Broadband Project [17] in 2004. This project deployed a small number of mesh devices [3] having in mind to provide the village with a reliable network infrastructure at relatively low-cost. Wray covers an area of around two square kilometers and Internet access is provided by means of a radio link (5.8GHz) which reaches Wray school main building, located on a hill. Then, wireless mesh nodes based on Locust Mesh firmware are located in strategic locations, chosen both due to geography and also due to expected location. Overall there are around 10 mesh nodes and it serves around 100 users, both from a residential and business coverage perspective. In order to assist in overcoming blind spots and also in providing better reliability, the Wray mesh runs the routing protocol *Ad-Hoc On demand Distance Vector (AODV)* protocol, which has been manually configured to ensure better network operation. Most of the nodes are claimed to achieve 3Mbps, restricted by manual policing in order to ensure fairness. Moreover, experiments [3] done in Wray state that the performance achieved by Wray users vary depending on equipment and location. End-users who installed an exterior antenna achieve around 2Mbps, while users relying on PCI or USB network cards achieve data rates as low as 0.5Mbps. All maintenance in the mesh network is done by community users. This is therefore a particular case of a UCN, in the sense that users are the heart of the network operation.

Generic Operation Bob has recently moved to Wray and would like to have Internet access. All he has to do is to ask the Wray volunteer management council for an USB device which assists him with the configuration to the closest mesh node. Bob's data is then transferred across the mesh network with the assistance of AODV, up to the Internet access located in the Wray school. Policing rules are enforced to ensure data fairness.

Resource management is ensured manually and enforced in a way that is fair based upon local usage. Each individual user in the mesh network is provided with a maximum data rate of 3Mbps.

Incentives in Wray relate to having Internet access in a remote area, at a low-cost. There is no specific need for mobility aspects. In Wray, there is a single MP - the community - which is also the VO. Hence, security is established by means of the regular Wi-Fi security ways, namely, WPA or WEP. Guests will have open access.

It should be noticed that in contrast with the previous examples of UCNs, there is not a global concept of bandwidth sharing in the sense that a group of users in a community is willing to share an existing access. In Wray, the MP is the community.

CuWIN The *Champaign-Urbana Community Wireless Network (CuWin)* [7] is a volunteer coalition composed of networking researchers-developers and community volunteers that are "committed to provide low-cost, non-proprietary, do-it-yourself, community-controlled alternatives to contemporary broadband models". The CuWIN vision consists in improving networking technology in a way that community of non-expertise people can deploy a wireless mesh network by themselves in order to satisfy their connectivity necessities.

CuWIN provides any regular user worldwide with the possibility to voluntarily host CuWIN nodes. In other words, upon demand CuWIN may provide their firmware to any user. In addition, CuWIN also sells a complete box solution, which includes CuWin firmware and hardware from Metrix (Metrix Mark II)[4].

CuWIN firmware (CuWinWare) is compatible with a reasonable number of chipsets, but however, it requires that the chipset of the wireless card to be supported by NetBSD ad-hoc drivers. CuWIN recommends installing on nodes that are expected to be static, e.g. old PCs. Installation can be performed by PXE booting, by CD, or by online updating.

Nodes run on 802.11b, channel 11 (defined at compile time). Moreover, CuWIN relies on a particular type of routing protocol, the *Hazy Sighted Link State (HSLS)* [5] protocol. HSLS is a link-state protocol developed by BBT technologies which uses both reactive and proactive routing to minimize route updates.In contrast to other link-state solutions, it prevents flooding the network by making changes in "far away" links become less relevant than changes on links "nearby". By applying the fuzzy-logic principles, propagation of link state changes is done in a quicker way to nearby nodes, than to nodes far away. This gives room for CuWIN to claim to scale up to thousands of nodes.

The CuWIN architecture is a two-layer hierarchical network. It contains a backhaul layer (identified by cuwireless.net) which is solely composed of CuWIN routers. The second layer is used by regular users (end-user layer, cuwireless), and may just contain off-the-shelf APs, or even another wireless networking solution. Internet access is provided by users (and organizations) belonging to the CuWIN community which are willing to share their service. They therefore become CuWIN gateways, from a mesh network perspective.

Currently, the most prominent projects that are based on CuWIN are the Urbana project, Wireless Ghana, Mesa Grande Reservation.

Generic Operation To setup a new wireless CuWin mesh network in a given community Bob must first download CuWin software [6] or acquire the CuWIN kit. Bob is a "do-it-yourself man" and opts for the software installation on an old desktop PC equipped with a wireless card that holds an Atheros chipset. After booting, Bob's PC becomes a CuWIN node. Bob is then part of the CuWin backhaul in his town and opts to share his own Internet access with the community. He then convinces a few other users around to join the network and hence the network grows steadily.

Ana is a visitor in town and wants to read her e-mail. She simply opens her PDA and can see the *cuwireless* SSID available, so she connects to it and immediately can use the available network.

CuWin provides no resource management at all, and hence the quality of the shared infrastructure depends upon the simultaneous number of users, as well as the type of traffic being used. Incentives to adhere to CuWin are free roaming and the possibility to expand the network at a low-cost. An interesting additional incentive is the promise of services in CuWin, such as a VoIP platform. Security is left to the user sharing his/her access. CuWin is an interesting platform in particular for communities willing to expand existing Internet access in remote areas.

FreiFunk Freifunk [8] is a non-commercial initiative which has as motto to provide free wireless access globally. The project is based upon mesh networking but adds the interesting feature of *picopeering-agreements (PPAs)* [1]. A PPA is an attempt to assist in allowing different wireless communities to interoperate, particularly having in mind free networks. Basic rules of a PPA are that an MP (owner of the PPA) must agree to provide free transit across the free network, and not to modify any data being transmitted; communication must be open; no warranties are provided. The PPA defines, in addition, terms of use which provide the MP with some flexibility in terms of formulating acceptance use policies. Freifunk provides users with a firmware (Freifunk Firmware, FFF) based on OpenWRT. The firmware originally included OLSR as the multihop routing protocol, a Web interface which provides AP configuration, as well as additional features such as traffic shaping and statistics, Internet gateway support. Today, FFF also provides support for Batman (in addition to OLSR).

Freifunk is therefore tailored for communities of users willing to share an Internet access, and there are several Freifunk communities, in particular in Germany. For instance, in 2004 the Berlin community consisted of 500 Freifunk APs, and Freifunk claimed having several thousand users accessing the Internet for free [9]. Freifunk claims 5945 users (shared APs) registered worldwide, being circa 2200 in Berlin alone.

Generic Operation Bob decides to become part of the local Freifunk municipality. Therefore he downloads the FFF and uploads it to his local and compatible AP. Once the AP is active, a new firewall configuration is provided, splitting the local network from the exterior network. In case NAT is present, Internet access is possibly by means of neighboring stations that announce Internet access. Bob does not own an Internet access, but Ana, his neighbor, does. She is willing to share that access with neighbors (such as Bob). Therefore, all she does is to plug her Internet access router to the AP where she installed the FFF. The FFF AP automatically receives a default gateway via DHCP, becomes a gateway, and relies on OLSR HNA4 to provide an announcement of the new gateway to other nodes on the network. The connection to the default gateway is continually checked using "arping". If the connection disappears, then the HNA4 announcement is discontinued.

Freifunk is an interesting and one of the oldest concepts of UCNs based on mesh networking. However, its main incentive relates to low-cost deployment. There is no security in place, nor any type of resource management features.

Open-Mesh Open-Mesh claims to be a “ ever-growing group of people dedicated to community-owned WiFi, not owned or controlled by any one corporate entity”. Open-Mesh products relate to the management platform required to assist an autonomous growth of community-owned mesh networks. Open-Mesh provides an AP/Access router based on different types of hardware and on the open source GPL *Routing OLSR and Batman INside (ROBIN)* [4] software platform. ROBIN is deployed on the operating system OpenWRT (Kamikaze version) and runs on any Atheros AP51 router. In terms of multihop routing, ROBIN gives the possibility to rely on *Better Approach to Mobile Ad-hoc Networking (BATMAN) [2].*

Generic Operation Bob decides to be a part of Open-Mesh. Therefore, he acquires an Open-Mesh AP or opts for just installing the Open-Mesh firmware in one existing compatible AP (e.g. Meraki, Ingenious, Ubiquiti). He then registers in Open-Mesh, to configure his mesh hotspot, by adjusting parameters such as SSID, location of owned APs, setting up WPA security, as well as the captive portal options. Moreover, Bob can specify MACs of the devices that can access a specific AP (SSID). Bob wants to create a mesh with 3 APs and hence registers the MAC of these APs, providing also a location for each. Then Bob configures the common (public) SSID for the three APs, and a private SSID (for his use only). Both SSIDs will provide the basis for secure networks, based on WPA (personal) credentials. Bob can also configure channel and fix the Wi-Fi rate to 5Mbps (or opt to have the regular auto adjustment).

Table [18] describes the main features of Open-Mesh. There is no resource management in terms of sharing the infrastructure. Cooperation incentives relate to the possibility to deploy a low-cost wireless network in a user-friendly way. Security is provided by means of WPA and the MP can also block clients by means of MAC filtering. Moreover, Open-Mesh gives the MP the possibility (Web-based) to configure its shared network and to have a basic perspective on the usage of the different nodes that compose the network.

NetSuKuKu The Netsuku project [16] envisions a completely autonomic network with no centralized control whatsoever, so that each node takes the same role on the network. It devises a set of protocols and architecture that should allow a network to scale to massive number of nodes and still require very little CPU and memory usage from each node.

Netsukuku relies on the end-user devices (personal computers) and is based on ad-hoc technology, meaning that, in order to be a part of the Netsukuku network, the user needs just to be at reach of another Netsukuku node and install the Netsukuku software. To allow the network to grow even more, in particular on its embryonic stage, it is possible for a node to be a part of the Netsukuku network through a VPN tunnel.

Netsukuku follows a fractal hierarchy in terms of topology, for the sake of both routing and naming efficiency. Nodes are grouped hierarchically into groups of 256 nodes, called a *gnode*. Then, gnodes are grouped in groups of 256 and so on, into n levels of hierarchy. The maximum level, n, depends on the number of addresses available, meaning that in IPv4 we have 2^{32} IPs, so n=4. Similarly, using IPv6 we have 2^{128} IPs, meaning n=16.

This hierarchical grouping of nodes was useful when creating both its own name resolution and routing protocol. The naming resolution scheme, named *A Netsukuku Domain Name Architecture (ANDNA)* [20] is designed as non-hierarchical and decentralized name resolution system and is a full replacement of the hierarchy *Domain Name System (DNS)* commonly used on the Internet. Moreover, Netsukuku relies on their own routing protocol, the *Quantum Shortest Path Netsukuku (QSPN) [21]*, which was specifically designed for the hierarchical topology of Netsukuku and is designed to be decentralized and demand very little resources from each node. From the perspective of naming and routing, gnodes represent true nodes on the topology, and within each topology level, routing performs independently.

The network formed by all Netsukuku nodes can be connected to the Internet, through some gateway nodes, but may also co-exist in a completely independent way. This means that Netsukuku nodes can communicate directly, and use any IP application over it.

Generic Operation Bob wants to expand its Internet access, and so, Bob installs the open-source Netsukuku software in his desktop computer. Bob's computer has an external high-gain antenna connected to its network card, and as a result, Bob can instantly connect to his Netsukuku neighbors, at reach of his wireless signal. The network is self-configured and there is nothing else that needs to be done in order for Bob to be able to communicate to every other Netsukuku node.

An interesting aspect for this UCN is that routing considers resource management based upon each node's available bandwidth. Incentives too cooperate in NetSukuku relate to the low-cost deployment in a completely plug&play way. In terms of security, Netsukuku follows the design principles of any mesh network: routers can sniff and misuse traffic. However, Netsukuku is developing a specific cryptographic layer (Carciofo) to provide end-to-end user anonymity and privacy to users, based on IP-in-IP tunneling. Interesting features of this particular case of a UCN are its decentralized naming scheme (ANDNA) and its particular routing protocol (QSPN). It should also be noticed that QSPN does not support mobile nodes and considers that networks are stable for a reasonable time (updates take several minutes), i.e., Netsukuku is not tailored for dynamic mesh networks, where nodes may join and/or leave frequently.

4.4 Mobile/Provider UCNs

This section provides a glimpse of the most recent category of UCNs. We described three products which assist the development of mobile-based UCNs. As shall be realized, the potential of this type of UCNs is still to be unveiled but what is clear is that the products here described will give a push to the deployment of UCNs.

MIFI MiFi [23][5] is a product (smart AP) of Novatel currently being offered by the operators Verizon and Sprint to their 3G customers, as a service differentiator. The product is tailored for users on the go, to provide shared connectivity based on an existing 3G access. Verizon provides an access management platform (Web based) which can be accessed by Wi-Fi. The MP can then check usage, perform trust management for the shared devices, and specify concrete rules for sharing connectivity. Hence, this is a product tailored for users which temporarily need to provide Internet access to a few devices on the go.

In 2011 Verizon and Sprint charged $59.99/month for a 3G service with Mifi, up to 5GB allowed [19]. Verizon also provides additional plans, e.g., daily

[5] stands for “My Wi-Fi”, read “maifai”.

vouchers. In terms of rates, Mifi 2200 [19] is constrained by the offered 3G rates and hence, users cannot profit from Wi-Fi data rates completely.

Generic Operation Bob is traveling with his family and spends the night at a hotel which has no Internet access. Bob has is Sprint 3G phone and can access the Internet. However, his wife Linda would also like to access the Internet. Hence, Bob activates his Mifi 2200, which provides a way to share his 3G phone Internet connection with Linda seamlessly.

MiFi does not integrate intelligentresource management. However, the MP can check the status of its subscription (data usage) and can manually perform admission control. Incentives to adopt Mifi simply relate to the sporadic need users may have to share Internet access based on 3G. This is not however a product tailored to allow global shared usage of existing private hotspots.

The security provided is simply based on MAC filtering, being the MP the one that states who can access his/her Mifi 2200. As additional features, Mifi 2200 provides an advanced policing and monitoring platform, which gives the means for the MP to prevent breaks in terms of subscription data rates limit.

JoikuSpot JoikuSpot [**?**] is a software-based solution that allows users to automatically deploy a UCN on their mobile phone. The software is in 2013 available in most mobile devices, and is free. In its regular version Joiku allows only HTTP/S connections and prevents to set up some hotspot configuration parameters (e.g. change ESSID name, turn on encryption), or in its full-featured "Premium" version that cost 9 euros. In addition, an optional module called JoikuBoost can be installed on top of JoikuSpot for allowing aggregation of multiple 3G connections.

Speakeasy Netshare Speakeasy, a Seattle based Service provider was one of the first providers allowing wireless access sharing. In 2003, Speakeasy unveiled the Netshare WiFi plan which had as main purpose to allow a user to share his/her access with neighbors. The incentive to become an MP would be a revenue from 50% in terms of access costs. Security was left to the MP, even though at the time there was a recommendation for using 128-bit WEP.

In addition to Internet access, Speakeasy would provide each new user with e-mail and newsgroup access, as well as backup dial-up access. Moreover, the sharing was available not only via Wi-Fi, but also via Ethernet, Homeplug, etc.

Netshare is therefore a first example of a provider based UCN, where an ISP specifically states that the MP is responsible for any infringement of the existing Internet access subscription. As can be seen by Table **??**, the main netshare incentive was revenue to the subscriber. The most relevant feature to cite is the fact that the provider would give each user (MP and regular users) e-mail and news access.

The ZON@FON Case The ZON@FON is a concrete example on the application of FON by means of an access provider. ZON is an alternative Portuguese access provider which holds several services, ranging from digital TV to Internet access. In terms of Internet access, ZON provides relies on advanced cable technology (optical fiber and Eurodocsis 3.0) to provide residential customers with up to 1Gbps. On the last hop to the Internet user, ZON provides different technologies, being Wi-Fi one of them. Recently, ZON partnered with FON to exclusively provide FON services in Portugal. Being a provider, ZON claims the deployment of around 100,000 ZON@FON hotspots in Portugal. The widespread deployment was achieved by providing each ZON subscriber with a specific AP/AR (based on the FON firmware, but updated to suit ZON's requirements), and also by having deployed a large number of APs in public locations, and specific neighborhoods in Portugal.

Even though technically ZON@FON follows the FON model, this is a concrete application of a UCN where the initiative is provided by the provider (access or service provider) and not by means of a user, or a community of users.

5 Comparative Analysis and Evolution Discussion

This section provides a comparative analysis of the five identified UCN categories. Such analysis is performed based on the main properties of UCNs, and on the different roles of users, MP and VO. The comparison is summarized in Table 1.

Let us start by explaining the differences in terms of who holds the VO role. In the hotspot category, the VO is a specific entity that manages credentials, initial authentication and AP registration. The same functionality is provided by the VO in the mesh-based model, but in this case the VO is normally a community of users. Similarly, in the social networking category, the VO is also a specific entity but its main responsibility is to ensure a secure exchange of credentials. In the case of the mobile-based and provider-based categories the role of VO is assigned to access operators. Therefore, the VO has a similar role across all categories. It has only a coordinating role and does not have any impact on the way traffic is transmitted in the communities or across the Internet. Moreover, the VO does not account for any end-to-end measures, such as data privacy or traceability. However, our understanding is that this role will evolve and the VO will, in the future, have responsibilities that go beyond initial setup and will become service differentiators, e.g. distributed mobility management across communities.

The set of MPs in the hotspot, social networking, and mobile/provider models fairly corresponds to the global user database, given that all users must share access to obtain a specific benefit. While in the mesh and mobile categories the MP set corresponds to a subset of the global community. Moreover, changes in the MP set are expected to be rare in most categories, being the exception to the rule the mobile-based category. A relevant aspect to mention is the impact that changes on the MP set may have on the overall network operation. In the hotspot model, and despite the fact that any user is an MP, the impact of changes to the MP set are not expected to affect significantly the network operation, given that such operation is tied to the Wi-Fi infrastructure mode, which splits the network operation into islands (hotspots). The same occurs in the social networking and provider-based categories. While in the mesh category, and despite the fact that MPs are a subset of the user universe, changes in the MP set are expected to bring high penalties to the network operation. This may possibly be counter-balanced due to the fact that most MPs are expected to exhibit a static behavior (roaming frequency may be low or scoped in nature).

In the mobile-based category changes to the MP set will introduce high variability into the network, given that users are expected to roam frequently - such variability is tied to the mobility pattern of all users.

From a global perspective, today, and due to the fact that the MP role is simply tied to the connectivity model, changes to the MP set are not significant from a global network perspective. However, the MP role is expected to evolve into a multi-user operation setting, where some forms of networking services, in particular in the control plane (e.g. AAA, mobility management) are to be sustained by the MP in cooperation with the access, as starts to happen when smart APs (such as Femtocells) are deployed.

Let us now provide some considerations in terms of adoption incentives. The promise of wider and free roaming is today the most common incentive. A second incentive observed is extra revenue or rebates for access cost. This incentive is more prominent in categories tied to the access stakeholders, e.g. provider-based categories, but it also appears in the social networking category. A third type of incentive is low-cost expansion of Internet access, and this is in fact the single incentive observed for examples that fall in the mesh category.

As these networks grow, incentives are also expected to evolve based upon new responsibilities that MPs may attain. For instance, incentives based on bandwidth tokens are feasible in a short-range time period, given that today such incentives are already present in a variety of collaborative tools, from an application layer perspective.

An interesting technical aspect is that most of the categories do not consider resource management even in simple forms. The categories that integrate some form of resource management are the ones where the VO is the provider - mobile-based and provider-based categories -, which is somewhat obvious given that the control of the network is still centralized and hence, easier to perform: management of network resources in the mobile-based and the provider-based models is based on subscription rules. Resource management is, however, a field which is essential to assist UCN growth. Providing MPs with the automatic capability to share bandwidth in a clever way is also an incentive that will be deployed in future models. Another relevant aspect to consider is that intelligent and dynamic resource management is a must to assist in preventing access technical infringements (e.g. going over the average rate stipulated in the Internet access subscription).

In terms of security and data privacy, today UCNs rely on the available schemes, namely WEP for the MP and, most of the times, open access to regular users. Moreover, there are categories (such as mesh-based) which do not even integrate security, simply leaving the choice to the user and advocating the use of application layer privacy tools. We argue that for future models it is necessary to ensure three basic properties: confidentiality, non-repudiation and traceability. These are aspects that can be dealt with by adequate trust management models.

Table 1. Comparison of the different UCN models.

	VO	**MP set**	**Resource Management**	**Cooperation Incentives**	**Mobility Management**	**Security Aspects**
Hotspot	- Specific entity. - manages credentials and initial authentication. - manages AP registration.	- All users. - Changes in the MP set are not frequent. - Changes in the MP set affect the network only partially.	- N/A	- Broader roaming. - Revenue for MPs	- N/A	- Mostly based upon private AP security (WEP).- security for the MP; open access for guests.
Mesh	- Community of users. - manages credentials and initial authentication. - manages AP registration.	- A subset - Changes in the MP set are not frequent. - Changes in the MO set affect all the network operation.	- N/A	- Low-cost network deployment.	N/A	- No integrated security.
Social	- Specific entity. - manages credentials for access to private APs following social networking.	- All users. - Changes in the MP set are not frequent. - Changes in the MP set affect the network partially.	- N/A	- Broader roaming. - Revenue for MPs.	N/A	- Third-party support for Wi-Fi (WEP, WPA) key exchange.
Mobile/Provider	Access or service provider - Provides any user with the possibility to share an existing 3G Internet access (limited sharing). - differentiates an existing service by relying on UCNs.	- All users - Changes in the MP set are expected to be frequent. - Changes in the MP set may bring heavy penalties to the network operation.	Based on subscription rules.	- On-the-go shared connectivity. - revenue broader roaming	3G roaming.	End-to-end if mobile access; otherwise requires VPN

6 UCNs Follow-up: Assumptions and Requirements

This section aims to identify a set of regulatory, social, and technical assumptions as well as requirements that must to be taken into account for the development of UCN solutions. The analysis of relevant assumptions is provided based on the four major conceptual properties of UCNs: connectivity sharing and relaying, cooperation, trust, and self-organization.

6.1 Connectivity Sharing and Relaying

Current examples of UCNs rely on one-hop wireless connectivity sharing by individual users, communities or organizations. In other words, an MP shares subscribed Internet access with specific communities. Such sharing can be based on equipment that is fixed in a specific place (e.g. residential household) or even just based on equipment carried by humans. Hence, MP elements may move while

Table 2. UCN Follow-up, asumptions and requirements.

	Assumptions	Requirements
Connectivity Sharing and Relaying	– MPs hold an Internet access subscription that is not regulated by the VO. – The set of MPs is essentially static over time. – Sharing is performed on specific communities (coordinated by VOs). – Sharing today is based on a single-hop, but future cases will incorporate multihop sharing (relaying across a few hops). – Equipment used in Internet access sharing can be fix (e.g. an AP) or mobile (devices carried by users). – The access operator does not control UCNs.	– Traceability across multihop sharing. – Security and non-repudiation. – Trust management. – Communities: UCNs must be able to support autonomic growing of communities of micro-operators, which decide for a common identity based on a set of cooperation parameters. – Software defined: UCNs deployed must be based upon low cost hardware of easy deployment, and software that is independent from radio technology, operating system, and devices. – Shared services: UCNs should provide a set of services, additionally to Internet connectivity, such as local DNS, Privacy, and data caching. – Coverage: UCNs may provide resource sharing within a few hops away from an Internet access point based on routing or simpler relaying methods. – Connectivity: UCNs should be able to keep active the offered services even in the presence of intermittent connectivity. Moreover sources and destinations may establish connectivity without the need to go to the access network. – Traffic: UCNs must be able to provide detailed accountability and traceability (e.g. useful for traffic imputation).
Cooperation	– Users are willing to share subscribed access against a specific benefit (currently, it is wider roaming, revenue, or rebates) – Network topology makes it possible to share subscribed access - networks are dense. – Users move across different locations (different APs)	– Technical incentives should be improved to assist in a win-win match for the sharers and the ones profiting from such sharing. Such incentives have to be considered from the end-user and from the access perspective. – UCNs must integrate mechanisms that reward adequately users that cooperate the most. – Scalability must be considered also from an adoption (spreading perspective). UCNs should integrate mechanisms to assist adhesion/adoption.
Trust Management	– UCNs only provide partial data confidentiality. – Current models disregard user anonymity aspects. – The MP is the accountable entity from an operator perspective.	– UCNs must allow sharing of Internet services based on well defined trust levels derived from social networking tool as well as from nodes networking behavior, and user's social behavior and interests. – UCNs should implement trust models that not only consider community beliefs, but are actually dependent upon surroundings and the level of confidentiality that the user expects on a specific moment and for specific application. For instance, trust models may be influenced by local conditions such as the degree of current connectivity and the current reputation level, as well as by external conditions such as the overhearing probability around a specific node. – UCNs must implement *grassroots* trust mechanisms, aiming to increase the scalability and robustness of the system, without being confined to a specific community – UCNs should implement reputation mechanisms (e.g., similar to the E-Bay model) to identify the networking behavior of nodes. – UCNs must ensure data confidentiality end-to-end and not only on the wireless link to the MPs. Confidentiality should be provided by mechanisms that do not reduce the user privacy. – Repudiation: UCNs must allow micro-operators to claim not having done a specific action (*repudiation*), otherwise he/she may see his Internet connection blocked or event have to deal with legal actions.
Self-organization	– UCNs form autonomously based on community behavior and driven by community needs. – Users are not fairly balanced across APs of MPs. – The MP set and user set varies frequently with time	– UCNs must be able to self-organize recurring to incentive schemes to ensure a smooth operation – UCNs must be able to provide a better usage of available resources, such as by taking advantage of aggregated backhaul capacity or load-balanced across the micro-providers in order to respect the traffic limits described in Internet subscription agreements – UCNs should be able to estimate its dynamic morphology, namely the number of users at specific periods of time, the node degree, as well as the average bandwidth that nodes can take advantage from.

sharing Internet access. Moreover, it is assumed that the MP already subscribes Internet access e.g. based on mobile, wireless, or fixed access technologies.

Another relevant aspect to consider is that the set of MPs today remains essentially static over time. In other words, the universe of users profiting from the sharing tends to be the same universe of users sharing, as we shall see with the examples provided. Sharing today is basically related to the offer of roaming services. By sharing access within a specific community, the user can profit from wider roaming.

6.2 Cooperation

Today's UCN cases are supported by the willingness of the end-user to become part of existing communities. Motivation to do so relates to the roaming incentive, and to the end-user's belief that the benefit of using UCNs is higher than the risk incurred. However, this is a fake sense of security, and with time, UCNs will evolve and users will become more intransigent in terms of incentives to cooperate.

6.3 Trust Management

Data privacy in UCNs is normally partial, given that it is only ensured on the wireless link and to the MPs. A user can of course cope with this gap by relying on specific privacy mechanisms, e.g., using some specific application or establishing a tunnel to a specific, trusted entity (e.g. a VPN to an enterprise). The flip-side of this is the related overhead both in terms of configuration/processing time , and in terms of data. It should also be noticed that despite the fact that the MP communication is protected, malicious user traffic may pass by the MP device (e.g. access point) and thus may result in serious violations. Another relevant aspect is traceability and non-repudiation, which becomes even more serious if one considers future multihop UCN scenarios. Trust management can assist in lowering the barriers of these concerns without the need to consider complex third-party certifying entities or revocators. Currently, trust within a specific UCN is confined to a specific community which is normally managed by a VO. In the future, trust models should not only consider community beliefs but actually be dependent upon surroundings, level of confidentiality that the user expects on a specific moment and for specific applications. Hence, the most adequate trust management models to consider in terms of UCNs are decentralized ones, where each peer holds specific trust values and metrics that other peers can access. In addition, ways to fight back selfishness of peers (fight back the *tragedy of the commons*) have to be considered, given that UCNs have a highly dynamic character in terms of who composes communities.

6.4 Self-organization

Self-organization is a key aspect in UCNs in particular due to the fact that the network operation is being placed closer to the user, and driven by community needs, and community network usage. Today, self-organization is applied in UCNs mostly for improving resource management aspects e.g. in case of offloading. Cooperation models require, however, self-organization to be addressed both from a network as well as from a user perspective, thus providing more robustness to UCNs, where the control functionality may be split across different physical devices which are not necessarily owned by a single operator, or even by an operator.

7 Summary and Conclusions

This paper provides an overview and categorization of UCN living-examples as a way to assist the robust development of these novel architectures and as a consequence to assist in a shift concerning Internet architectural design.

A first conclusion to draw is that there is a clear paradigm shift due to cooperation amongst Internet communities which is changing the network operation and giving rise to new networking opportunities. A second conclusion is that there are clear technical and economic limitations to today's UCNs. Technical aspects to improve relate to adequate resource management, mobility and security. From an access perspective there are technical advantages that must also be considered, such as solutions to keep traffic "local" (confined to specific communities) or even methods to make networks more robust by exploring cooperative networking. Economic limitations of these architectures are today tightly related to the lack of understanding in terms of applicable business models. Therefore, a key aspect to analyze are ways to model incentives in a way that becomes profitable to both the individual user and the community, as well as to the access.

Research work in this field should consider how to optimize available resources (bandwidth and energy);how to devise trust models to lower operational complexity due to a need to reinforce security (traceability and liability); how to define incentive plans to adhere to these novel architectures.

Acknowledgements

We thank all of the authors that contributed to the white paper on which this paper was based, report number SITI-TR-11-03 (2011): Rute C. Sofia, Paulo Mendes, Waldir Moreira Junior, Andréa Ribeiro, Saulo Queiroz, Antonio Oliveira Junior, Tauseef Jamal, Namusale Chama and Luís Carvalho.

References

1. Pico peering agreement v1.0. http://www.picopeer.net/PPA-en.html.
2. Better approach to mobile ad-hoc networking (b.a.t.m.a.n.). *IETF draft (Expired)*, 2008.
3. J. Ishmael, S. Bury, D. Pezaros, N. Race. Deploying rural community wireless mesh networks. *IEEE Internet Computing*, 12:22–29, August 2008.
4. Antonio Anselmi. Robin - open source wireless mesh networking. http://robin-mesh.wik.is/, November 2009.
5. C. Santivanez and R. Ramanathan. Hazy sighted link state (hsls) routing: A scalable link state algorithm. *BBN Technical Memo BBN-TM-1301, BBN Technologies, Cambridge, MA, USA*, August 2001.
6. CuWin. Cuwin ware kit. http://sourceforge.net/projects/wireless/files/wireless/, 2009.
7. CuWin. Community wireless solutions. http://cuwireless.net/, 2009.
8. Freifunk. Freifunk community. http://start.freifunk.net/, 2006.
9. Freifunk. Freifunk.net - a successful do-it-yourself approach for building wireless community networks in germany. http://start.freifunk.net/, October 2006.
10. D.D.Clark J.H. Saltzer, D.P.Reed. End-to-end arguments in system design. *ACM TOCS*, 2:277–288, 1084.
11. Linspot. Linspot. http://www.linspot.com/, 2009.
12. KeyWifi LLC. Keywifi: Unlocking hotspots near you. http://keywifi.com/.
13. FON Wireless Ltd. Fon. http://www.fon.com, 2009.
14. M. Solarski, P. Vidales, O. Schneider, P. Zerfos, J.P. Singh. An experimental evaluation of urban networking using ieee 802.11 technology. *1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks*, pages 1–10, 2006.
15. MP-MasterPlanet Oy Matti KiviÃ¶. Openspark. http://www.openspark.fi, 2009.
16. Netsukuku. Netsukuku - close the world, txen eht nepo -. http://netsukuku.freaknet.org/, 2009.
17. Network Research & Special Projects Units, University of Lancaster. Wray broadband project, 2006.
18. Open-Mesh. Open-mesh, ultra low cost wifi. http://www.open-mesh.com/store/.
19. WiFi Planet. Novatel wireless mifi 2200 for cdma 1x ev-do networks. http://www.wi-fiplanet.com/reviews/article.php/3824351, June 2009.
20. Netsukuku Project. Andna - a netsukuku domain name architecture, manual. http://netsukuku.freaknet.org/doc/manuals/andna.
21. Netsukuku Project. The qspn. Technical report, September 2009.
22. P. Mendes R. Sofia. User-provided networks: Consumer as provider. *IEEE Communication Magazines, Feature Topic on Consumer Communications and Networking - Gaming and Entertainment*, 46:86–91, 2008.
23. Verizon. Mifi 2200, intelligent mobile hotspot. $http : //www.verizonwireless.com/b2c/mobilebroadband/?page = products_{m}ifi$.
24. Wray Village. Wray community communications. http://www.wrayvillage.co.uk/wraycomcomhome.htm.
25. Wifi.com. Whisher. http://www.whisher.com/, 2009.
26. S. Kawade; J.-W. Van Bloem; V.S. Abhayawardhana; D. Wisely. Sharing your urban residential wifi (ur-wifi). *IEEE 63rd Vehicular Technology Conference. VTC 2006-Spring.*, 1:162 – 166, 2006.